PHILLIP A. TALBERT
United States Attorney
TARA AMIN
Assistant United States Attorney
501 I Street, Suite 10-100
Sacramento, CA 95814
Telephone: (916) 554-2700
Facsimile: (916) 554-2900

AMANDA N. LISKAMM
Director
RACHAEL L. DOUD
Assistant Director
ANDREW K. CRAWFORD
FRANCISCO L. UNGER
Trial Attorneys
Consumer Protection Branch
Civil Division
U.S. Department of Justice
450 5th Street, NW
Washington, DC 20530
Telephone: (202) 451-7301
Email: andrew.k.crawford@usdoj.gov

Attorneys for Plaintiff United States of America

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

United States of America,

Plaintiff,

v.

CB SURETY LLC, a North Carolina limited liability company; PEAK BAKERY LLC, a North Carolina limited liability company; CASCADES POINTE AT CLEMSON, LLC, a South Carolina limited liability company; KP TESTING, LLC, a Virginia limited liability company; THOMAS EIDE, in his individual capacity and as an officer of various corporate defendants; TRAVIS SMITH, in his individual capacity and as an officer of various corporate

Civil Case No. 2:23-cv-2812 TLN DB

COMPLAINT FOR TEMPORARY RESTRAINING ORDER, PRELIMINARY AND PERMANENT INJUNCTIONS, AND OTHER EQUITABLE RELIEF

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT
DATED _____

defendants; ARIC GASTWIRTH, in his individual capacity and as an officer of various corporate defendants; RESELLER CONSULTANTS, INC., a Nevada corporation; AMBRAGOLD, INC., a Florida corporation; STEPHEN CHRISTOPHER, in his individual capacity and as an officer of various corporate defendants; MOTION MEDIA MARKETING, INC., a California corporation; SJC FINANCIAL SERVICES, INC., a California corporation; BRYAN BASS, in his individual capacity and as an officer of various corporate defendants; THINK PROCESSING LLC, a Wyoming corporation; BASS BUSINESS CONSULTANTS, an India corporation.

Defendants.

Plaintiff, the United States of America, by and through the undersigned attorneys, hereby alleges as follows:

I. NATURE OF THIS ACTION

1. The United States brings this action for a temporary restraining order, preliminary and permanent injunctions, and other equitable relief pursuant to 18 U.S.C. § 1345 to enjoin the ongoing commission of criminal wire fraud and bank fraud and conspiracy to commit those offenses in violation of 18 U.S.C. §§ 1343, 1344, and 1349. The United States seeks to prevent continuing and substantial injury to the victims of Defendants' fraud.

2. Defendants are members of a transnational network of fraudsters engaged in an ongoing bank and wire fraud scheme that since at least 2017 has targeted and victimized financial institutions and consumers across the United States.

3. Defendants process payments for merchant clients that are engaged in fraudulent, illegal, or high-risk activities including the sale of illegal drugs, gambling, technical-support scams, and making unauthorized charges to consumers' bank and credit card accounts. Defendants operate the scheme by creating and controlling sham companies to launder money

through seemingly legitimate but fake companies to give their merchant clients access to the banking system.

4. Defendants also use sham transactions to decrease the apparent rate of "chargebacks"—*i.e.*, instances in which transactions are reversed by the consumers' bank because, for example, the consumer has reported the charge as unauthorized—by artificially inflating the total number of charges a merchant appears to process. This deceptive tactic allows Defendants' merchant clients to maintain bank accounts despite high chargeback rates, which merchant banks track as a key indicator of fraud.

5. Over the course of the scheme, Defendants have processed many millions of dollars in payments. Between July 2020 and June 2023, for example, Defendants, through transaction laundering, processed approximately $97 million in payments for their merchant clients, thereby causing losses to consumers, and fraudulently causing federally insured banks to risk substantial losses.

6. For the reasons stated herein, the United States requests injunctive relief pursuant to 18 U.S.C. § 1345 to put a stop to Defendants' ongoing scheme and prevent them from causing further harm.

II. JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under 18 U.S.C. § 1345 and 28 U.S.C. §§ 1331 and 1345 because Defendants' fraud scheme targets victims in the United States and in this District.

8. The United States District Court for the Eastern District of California is a proper venue for this action under 28 U.S.C. §§ 1391(b) and 1391(c) because CB Surety LLC maintains an office located in the Eastern District of California, and because it continues to operate from this District.

III. PARTIES

9. Plaintiff is the United States of America.

CB Surety Defendants

10. **Defendant Thomas Eide** maintains residences in this District and the District of South Carolina. In connection with the matters alleged herein, Eide transacts and has transacted business in this District and throughout the United States. Defendant Eide controls Defendants CB Surety LLC, Peak Bakery LLC, Cascades Pointe at Clemson, LLC, and KP Testing, LLC.

11. **Defendant Travis Smith** is a resident of Texas. In connection with the matters alleged herein, Smith transacts and has transacted business in this District and throughout the United States. Defendant Smith controls Defendants CB Surety LLC, Peak Bakery LLC, Cascades Pointe at Clemson, LLC, and KP Testing, LLC.

12. **Defendant CB Surety LLC** ("CB Surety") is a North Carolina company with its registered address at 4030 Wake Forest Rd Ste 349, Raleigh, North Carolina 27609, and its principal place of business at 3079 Harrison Avenue #10, South Lake Tahoe, California 96150. Defendants Eide and Smith are its managers. In connection with the matters alleged herein, CB Surety LLC transacts and has transacted business in this District and throughout the United States. CB Surety also does business as Knox Secure and Prepaid Friends.

13. **Defendant Peak Bakery LLC** is a North Carolina company with its registered address at 4030 Wake Forest Road Ste 349, Raleigh, North Carolina 27609, and its principal office at 1919 McKinney Ave Ste 100, Dallas, Texas 75201. Defendant Smith is its manager. Defendant Peak Bakery LLC makes and receives payments on behalf of Defendant CB Surety LLC. In connection with the matters alleged herein, Peak Bakery LLC transacts and has transacted business in this District and throughout the United States.

14. **Defendant Cascades Pointe at Clemson, LLC**, is a South Carolina limited liability company with its registered address at 2 Office Park Court, Suite 103, Columbia, South Carolina, 29223. Defendant Eide is one of its managers. Defendant Cascades Pointe at Clemson, LLC makes and receives payments on behalf of Defendant CB Surety LLC. In connection with the matters alleged herein, Cascades Pointe at Clemson LLC transacts and has transacted business in this District and throughout the United States.

15. **Defendant KP Testing, LLC** is a Virginia limited liability company with its principal office at 409 East Main Street, Suite 205, Richmond, Virginia 23219. Defendant Smith is its manager. Defendant KP Testing, LLC makes and receives payments on behalf of Defendant CB Surety LLC. In connection with the matters alleged herein, KP Testing, LLC transacts and has transacted business in this District and throughout the United States.

Merchant Account Broker Defendants

16. **Defendant Stephen Christopher** is a resident of California. In connection with the matters alleged herein, Christopher transacts and has transacted business in this District and throughout the United States. Defendant Christopher controls Defendants Motion Media Marketing, Inc. and SJC Financial Services Inc.

17. **Defendant Motion Media Marketing Inc.** is a California company with its registered address at 14144 Mazatlan Court, Poway, California 92064. Stephen Christopher is the registered agent. In connection with the matters alleged herein, Motion Media Marketing Inc. transacts and has transacted business in this District and throughout the United States.

18. **Defendant SJC Financial Services Inc.** was a California company with its registered address at 13940 Umbria Way, Poway, California 92064. Stephen Christopher was the registered agent. The activities of SJC Financial Services, Inc. are now conducted by Motion Media Marketing Inc. In connection with the matters alleged herein, SJC Financial Services Inc. has transacted business in this District and throughout the United States.

Sham Entity Recruiter Defendants

19. **Defendant Aric Gastwirth** is a resident of Nevada. In connection with the matters alleged herein, Gastwirth transacts and has transacted business in this District and throughout the United States. Defendant Gastwirth controls Defendants Reseller Consultants, Inc. and Ambragold, Inc.

20. **Defendant Reseller Consultants, Inc.** is a Nevada company with its registered address at 3773 Howard Hughes Parkway, Ste 500S, Las Vegas, Nevada 89169. Its director is

Annette Goldstein. In connection with the matters alleged herein, Reseller Consultants, Inc. transacts and has transacted business in this District and throughout the United States.

21. **Defendant Ambragold, Inc.** was a Florida corporation with its principal address at 9835-16 Lake Worth Road #122 Lake Worth, Florida 33467. Its president and director was Annette Goldstein. In May 2022, Articles of Dissolution filed with the Secretary of State of Florida were signed by Aric Gastwirth. The activities of Ambragold, Inc. are now conducted by Reseller Consultants, Inc. In connection with the matters alleged herein, Ambragold, Inc. has transacted business in this District and throughout the United States.

Merchant Account Servicer Defendants

22. **Defendant Bryan Bass** is a resident of India. In connection with the matters alleged herein, Bass transacts and has transacted business in this District and throughout the United States. Defendant Bass controls Defendants Think Processing LLC and Bass Business Consultants.

23. **Think Processing LLC** is a Wyoming corporation with its registered address at 1309 Coffeen Avenue, Suite 1200, Sheridan, Wyoming 82801. Its sole member is Defendant Bass. In connection with the matters alleged herein, Think Processing LLC transacts and has transacted business in this District and throughout the United States.

24. **Bass Business Consultants** is a corporation headquartered in Punjab, India. Defendant Bryan Bass is its manager. In connection with the matters alleged herein, Bass Business Consultants transacts and has transacted business in this District and throughout the United States.

25. In connection with the matters alleged herein, all Defendants have participated in a wire fraud and bank fraud scheme, and conspired with each other to participate in a wire fraud and bank fraud scheme, that targets individuals and entities in the United States, including in this District.

IV. DEFENDANTS' ONGOING FRAUD SCHEME

Relevant Background on Payment Card Transactions

26. When a consumer pays a merchant for a good or service using a payment card such as a credit or debit card, several entities are involved in processing the transaction so that payments can get from the consumer's bank account (also known as the "issuing bank") to the merchant's bank account (also known as the "acquiring bank").

27. Consumers obtain payment cards through their issuing bank. The issuing bank issues payment cards associated with a card network—such as Visa, Mastercard, American Express, or Discover. Businesses that wish to accept a consumer's payment card payments must apply for a merchant account with an acquiring bank.

28. When a consumer uses their card to pay for a good or service, the merchant receives the payment through a card reading device or a merchant's website, known as a "payment gateway." A payment processor, which often operates the payment gateway device or software, then routes the card data to the card networks and banks. If the consumer's issuing bank reports that the card is valid and there are sufficient funds or credit for the transaction, the issuing bank holds an authorization on the consumer's account for the transaction and sends an approval message to the payment gateway used by the merchant. This process typically happens near-instantaneously.

Financial Institution Diligence Prior to Opening Merchant Accounts

29. Before accepting a merchant's application for a merchant bank account, acquiring banks and third-party intermediaries, such as payment processors, typically assess the merchant's business and the level of risk in working with the merchant. Such an assessment may include a review of a merchant's business history; financial stability; the kinds of products or services offered; the risk of the industry in which the merchant operates; the volume of the merchant's transactions; the merchant's billing, credit, and return policies; and the merchant's "chargeback" rate, which indicates what percentage of the merchant's sales result in chargebacks.

Ongoing Monitoring

30. Card networks require that acquiring banks regularly monitor their merchant customers to detect suspicious activity and ensure that their merchant customers are engaged in businesses that are not illegal or in violation of the card network's policies. If acquiring banks fail to do so, the card networks may fine the acquiring bank or revoke their ability to receive payments from network-affiliated payment cards.

31. When an acquiring bank discovers that a merchant is engaged in fraudulent, illegal, or prohibited activity, it will typically close the merchant's bank account.

32. Card networks and payment processors maintain lists of businesses whose accounts have been closed after they were discovered to be engaged in fraudulent, illegal, or prohibited activities. These lists are variously known as the MATCH List, the Terminated Merchant File ("TMF"), and the Group Negative File.

Chargebacks

33. A "chargeback" occurs when a customer disputes a payment card transaction and asks their issuing bank to reverse the charge. A customer may do so on the grounds that the charge was unauthorized or fraudulent, among other reasons.

34. After a consumer initiates a chargeback, the issuing bank will typically credit the consumer's account and, through the payment processor, deduct the value of this credit from the merchant's account with the acquiring bank.

35. Credit card networks and acquiring banks typically monitor chargebacks by calculating a "chargeback rate." The chargeback rate is the total number of chargebacks in a month divided by the total number of transactions in that month. For example, if a merchant had five chargebacks out of 100 total transactions in a single month, the merchant's chargeback rate for that month would be five percent.

36. Generally, card networks begin to impose additional requirements and/or penalties on a merchant when a chargeback rate exceeds one to three percent. For example, Mastercard has an Excessive Chargeback Monitoring Program by which it monitors merchants'

chargeback rates. If a merchant's chargeback rate is above 1.5 percent for an extended period, Mastercard may assess fees on the acquiring bank.

37. These card network policies create incentives for acquiring banks to review and impose higher fees on or close accounts of merchants whose chargeback rates exceed the card network's acceptable rate. As a result, acquiring banks generally will not accept merchants with high chargeback rates and will seek to detect high chargeback rates during their underwriting.

Risk of Loss

38. Chargebacks subject acquiring banks and payment processors to the risk of loss because a merchant's account at an acquiring bank serves as a line of credit. Liabilities incurred by a merchant can become a credit exposure to an acquiring bank if they exceed the merchant's reserves. In the event of a chargeback, the acquiring bank and/or payment processor will refund a consumer. In turn, the acquiring bank expects the merchant to pay the bank for the chargebacks they incur. Therefore, chargebacks can become a credit exposure to an acquiring bank if a merchant is unwilling or unable to pay for the chargebacks. It also can be costly to acquiring banks to investigate and resolve chargebacks.

39. Further, high chargeback rates can expose acquiring banks to liability for facilitating fraudulent, deceptive, or otherwise unlawful conduct and cause the merchant banks reputational harm. Additionally, if the merchant has a chargeback rate that exceeds a card network's policy, or if the merchant engages in practices that contravene a card network's policy, the acquiring bank may incur financial penalties from the card network.

Structure of the Scheme

40. Defendants defraud banks and consumers by engaging in two core, related tactics to enable merchants engaged in fraudulent, illegal, or high-risk activities to obtain and maintain the capacity to receive card payments. Both tactics entail defrauding financial institutions.

41. *First*, Defendants help merchants that would otherwise be unable to obtain or have difficulty obtaining merchant bank accounts obtain and maintain such accounts by using sham companies controlled by the CB Surety Defendants. Defendants use these sham companies

to misrepresent the nature of the merchant clients' businesses and the nature of the transactions passing through the merchant clients' accounts ("transaction laundering" and/or the "transaction-laundering tactic").

42. *Second*, to help their merchant clients maintain merchant bank accounts, Defendants conduct sham transactions to artificially lower chargeback rates (the "chargeback-reduction tactic").

43. Absent these transaction-laundering and chargeback-reduction tactics, Defendants' merchant clients that are engaged in fraudulent, illegal, or high-risk businesses would not be able to access the United States' financial system or would be considered so high risk that access to the United States' financial system could be prohibitively expensive.

Overview of Defendants' Roles in the Scheme

44. Defendants Eide and Smith are organizers of the fraud scheme and conspire with others to recruit merchant clients, create, and control sham companies, and conduct sham transactions. Defendants CB Surety, Peak Bakery, Cascades Pointe at Clemson, and KP Testing are companies controlled by Defendants Eide and Smith (collectively, "CB Surety Defendants"). Peak Bakery, Cascades Pointe at Clemson, and KP Testing were created for the purpose of disguising scheme proceeds passing between CB Surety and other members of the scheme. For example, a September 2022 bank statement for CB Surety's bank account reflects thousands of dollars in payments from KP Testing, Peak Bakery, and Cascades Pointe at Clemson for office space and commissions paid to Defendant Bass. Likewise, a January 2023 bank account statement for Peak Bakery reflects thousands of dollars in payments from CB Surety controlled sham companies and thousands of dollars in payments to other CB Surety controlled sham companies, KP Testing, Cascades Pointe at Clemson, Reseller Consultants, and Eide.

45. Defendant Stephen Christopher and his businesses, Defendants Motion Media Marketing Inc. and SJC Financial Services Inc. (collectively, "Merchant Account Broker Defendants"), recruit and onboard merchants engaged in fraudulent, illegal, or high-risk

activities. The Merchant Account Broker Defendants also act as liaisons between CB Surety Defendants and their merchant clients.

46. Defendant Aric Gastwirth and his businesses, Defendants Reseller Consultants, Inc. and Ambragold, Inc. (collectively, the "Sham Entity Recruiter Defendants"), recruit and onboard individuals to serve as straw owners of sham companies that CB Surety controls and uses to disguise the identity of its merchant clients engaged in fraudulent, illegal, or high-risk activities. Gastwirth and his business also facilitate payments to the straw owners of the sham companies. For example, invoices sent by Gastwirth in the name of Ambragold, and later Reseller, include charges from Ambragold and Reseller for items such as "LLC Formation fees." This charge and others reflect Gastwirth's efforts, through Ambragold and Reseller, to create and maintain the sham companies through which Defendants launder transactions.

47. Defendant Bryan Bass and his businesses, Defendants Bass Business Consultants and Think Processing LLC (collectively, the "Merchant Account Servicer Defendants"), service the merchant clients and sham companies to help conceal the fraud. This involves fielding complaints from consumers and inquiries from banks and payment processors performing diligence on the sham companies. Defendant Bass also uses Think Processing LLC to recruit merchants engaged in high-risk or illegal activities, to receive laundered proceeds from sham companies, and to transfer those proceeds to Defendants and their merchant clients. For example, Defendant Smith maintains an Excel workbook with a spreadsheet named "Bass" in which payments from several online casinos are split between CB Surety and Think Processing. As another example, in May 2023, Bass sent an invoice to a merchant client in the name of Think Processing for various services including "Chargeback, Gateway and MID management" and "Account Management." The merchant client receiving the invoice purports to be a travel agency but has been the subject of numerous Federal Trade Commission complaints for being a scam.

Transaction-Laundering Tactic

Recruitment of Merchant Clients Engaged in Fraudulent, Illegal, or High-Risk Activities

48. Defendants recruit merchant clients engaged in fraudulent, illegal, or high-risk businesses to use their transaction-laundering services. Defendants Stephen Christopher and Bryan Bass are responsible for the recruitment.

49. Defendants Christopher and Bass recruit merchant clients by advertising their ability to help merchants access the banking system, which attracts merchants involved in the sale of illegal drugs, gambling, and technical-support scams, and other fraudulent business activities. For example, Bass runs a Wyoming corporation, Think Processing LLC, through which he recruits merchants engaged in high-risk or fraudulent activities to the scheme. In keeping with Think Processing LLC's role in the scheme, CB Surety payment logs reflect various payments to it for help in processing new merchants. Christopher, meanwhile, entered into a May 2017 agreement with CB Surety stating terms under which Christopher would work for CB Surety as a merchant broker helping in the sale and marketing of CB Surety's services. Both Bass and Christopher have recruited merchants engaged in illegal or high-risk activities to the scheme, such as merchants engaged in remote technical support scams and other fraudulent activities.

50. CB Surety Defendants are aware of the nature of their clients' businesses, including their clients conducting unauthorized charges, and have supported these businesses for years.

51. For example, on July 29, 2020, Eide forwarded to Smith a voicemail message from a California victim, J.G., regarding numerous fraudulent charges against J.G.'s accounts. J.G. noted, in a separate email sent to numerous email accounts controlled by Eide and Smith that were associated with the sham companies they controlled, that she had "no affiliation, no orders, or any accounts with" the merchants debiting her accounts and those charges were "NOT authorized by" her. In fact, these fraudulent charges were generated by Defendants' merchant clients using Defendants' transaction-laundering services.

52. J.G.'s experience is typical. From at least June 2020 through June 2023, CB Surety employees and agents compiled and circulated spreadsheets on an almost daily basis detailing consumers' attempts to contact the sham companies. In 2020, the complaints for just one day included, among others, the following:

> Your [sic] attempting to take an amount out of my checking and the banks [sic] putting a hold on it. So I speak to someone please. Give me a call.
>
> I received a withdrawal on a financial account I have from "CHS*Glorymar Men CLEVELAND TN" .... Either you have sold your name to be used for overseas transactions by gambling or otherwise illegal entities, or someone has stolen it. This is fraud in either scenario, so I wanted to reach out and see if you knew about this. Please contact me back so I know how to approach it with my bank. Thank you.
>
> Yes, hi. I got a text message saying I ordered something through your company and no I did not. So whatever this order is. I need you to cash refund me the $56 that you're supposed to be charging me. If you could please give me a call back.

53. In June 2023, the complaints for just one day included, among others, the following:

> She got charged twice , the first one is on 6th of June for $145 and the second was on the 25th of May for $145, Customer did not recognize the transaction. Requesting for refund
>
> Customer did not recognize the transaction. Requesting for refund, Remove her card
>
> She got charged from different companies, Customer did not recognize the transaction. Requesting for refund
>
> Called 2nd time, Customer did not recognize the transaction. Requesting for refund

Defendants' Recruitment of Straw Owners and Creation of Sham Companies

54. To create the sham companies to disguise the true nature of Defendants' merchant client businesses, Defendant Aric Gastwirth has used his companies to recruit straw owners.

Gastwirth and Reseller Consultants solicit from potential straw owners the personal information needed to obtain merchant accounts and form limited liability corporations ("LLCs").

55. In exchange for the promise of a small monthly payment, potential straw owners agree to, among other things, open bank accounts in the names of LLCs, open private mailboxes at commercial mail receiving agencies ("CRMAs") to serve as "virtual offices," and sign and return applications and documents to banks to obtain merchant bank accounts.

56. Gastwirth and Reseller Consultants generally incorporate two LLCs in the name of each straw owner, typically corresponding alphabetically with the straw owner's first name and consisting of three seemingly unrelated words followed by the designation LLC. This naming convention apparently helps Defendants keep track of which sham company is affiliated with which straw owner.

57. At the direction of Gastwirth and Reseller Consultants, straw owners open private mailboxes at CMRAs, such as The UPS Store, that serve as the sham companies' business addresses. The straw owners also open a checking account for each of their sham companies, and sign various sham agreements, typically for warehouse and fulfillment, call center services, and chargeback mitigation. The sham companies do not sell any goods or services and therefore do not in fact use warehouse or fulfillment services; however, acquiring banks rely on merchants having contracted such services to substantiate that the merchant applicant operates a legitimate business.

58. Defendants then purchase internet domains similar to the name of each of the sham companies. These internet domains are later integrated with CB Surety's technology platform, which links payments made to its merchant clients with its sham companies. This linking enables a transaction made to or by a high-risk, illegal, or fraudulent merchant client to appear to the acquiring bank as if it was made to or by the sham company for a legitimate purpose. Each of these sham companies' internet domains corresponds with an application for merchant accounts submitted by Defendants to banks.

59. The goods and services advertised on the sham companies' websites do not exist. Instead, they are front websites that the Defendants use to substantiate applications for merchant accounts. Defendants use these front websites to convince banks that the sham companies sell real goods and services.

60. Defendants then misrepresent the nature of the merchant clients' businesses to financial institutions, using the sham companies and websites to substantiate their claims. For example, in September 2019, Defendant Smith sent an email to two merchant account brokers acknowledging that the sham company "Diamani Urban Ventures" is a "a new corp for Sebastian's group. So they are Kratom." (Kratom is a drug with psychoactive ingredients. Although it is not regulated federally, it is illegal to buy, use, or sell in several states, and it is regulated in other states.) In a separate email, Defendant Smith wrote, "Here is a new merchant we have. They sell Kratom, will this do for the inventory pictures?" and asked for feedback on the site www.diamaniurban.com. The attached "inventory pictures" depicted a leather handbag and a balance board or hover board. In a merchant processing application to BMO Harris Bank, N.A., an acquiring bank, the corporate officer on behalf of Diamani Urban Ventures was listed as Desta Yalew and there was no mention of "Sebastian" or "Kratom." The application described the "Merchandise/Services Sold" as "electronic travel boards, Hoverboards, Scooters, Bikes."

61. Defendant Gastwirth, through Reseller Consultants, invoices Merchant Account Broker Defendants for processing fees, LLC formation fees, and registered agent fees, among other items.

Defendants' Control of the Sham Companies

62. Defendants control the sham companies, including their means of communication with third parties, their corporate actions, and their finances. At the CB Surety Defendants' direction, the Merchant Account Servicer Defendants provide services, including fielding complaints and inquiries from consumers intended to help conceal the fraud.

63. Each website created by Defendants to substantiate the fraudulent merchant account applications lists a "support email" as the email contact for the company. For example,

the sham company Aasher Young Creations LLC has numerous website domains, including aasherdecor.com, and its email contact address is support@aasherdecor.com. The CB Surety Defendants and Merchant Account Servicer Defendants control these email addresses and use them to communicate with third parties, including financial institutions, payment processors, and consumers, in the name of the sham companies.

64. The CB Surety Defendants and the Merchant Account Servicer Defendants also control Gmail accounts in the names of the sham companies. For example, CB Surety maintains a master spreadsheet compiling Gmail account information for the scheme's sham companies, including address, password, and password recovery information to facilitate control of the accounts. Similarly, another CB Surety master file demonstrates that CB Surety implemented the same passwords across many sham company Gmail accounts to simplify its control and use of them. Emails addresses are an important way that acquiring banks substantiate the existence of merchant applicants. The Merchant Account Servicer Defendants use the sham companies' email addresses to field customer complaints and to respond to inquiries from acquiring banks or other financial institutions performing diligence to confirm the authenticity of the sham company.

65. For example, in April 2021, a fraud analyst from Elavon (a payment processor and wholly owned subsidiary of U.S. Bank, which is insured by the Federal Deposit Insurance Corporation) emailed the straw owner email address techuengcheng1143@gmail.com and indicated that the merchant account for Tianny Mighty Adventures LLC, a sham business that does business as Tianny Bike Helmets, was under review. The fraud analyst asked where Tianny Bike Helmets' inventory was stored, for a photo of the inventory as well as a receipt showing the business name and address, and a bill with the business name and address. In response, techuengcheng1143@gmail.com claimed that Tianny Bike Helmets could not provide any photos because it was an e-commerce business and did not have access to its inventory. Techuengcheng1143@gmail.com attached an invoice of a transaction that it claimed substantiated its business name and address. The attached invoice indicated that on April 1, 2021, a customer, T.H., bought from Tianny Bike Helmets an item called "Synthe Helmet Pad

Set" and paid a total of $50. A spreadsheet from Defendant Smith's email account indicates that the $50 charge to T.H. was a charge by Palau Holdings NV, which owns and operates online casinos.

66. The CB Surety Defendants use an Excel spreadsheet titled "_MASTER_" to track a Gmail address, Google Voice phone number, and password for each straw owner and sham company.

67. Defendants forward incoming phone calls to the phone numbers associated with the sham companies to Google Voice numbers controlled by Defendants and the Merchant Account Servicer Defendants so that they can field phone calls made to the sham companies and monitor consumer complaints.

Applying for and Maintaining Merchant Accounts

68. After Gastwirth and Reseller Consultants recruit straw owners and create sham companies in the names of straw owners that Defendants in fact control, Defendants initiate numerous applications for merchant accounts, which are required for the merchants to process card payments, using the trade names of each of the sham companies. In those applications, Defendants do not disclose that Defendants, and not the straw owners, operate the sham companies; that Defendants' merchant clients, and not the sham companies, will be using the accounts; or that the accounts will be used to facilitate transactions connected to high-risk, fraudulent, or illegal activities such as drug sales, gambling, and technical-support fraud. As noted above, Defendants substantiate their misrepresentations by listing the fake websites they have created in the various trade names of the sham companies.

69. To further maintain the fraud, as noted above, the CB Surety and Merchant Account Servicer Defendants field customer complaints and respond to inquiries from payment processors performing diligence to confirm the authenticity of the sham companies. For example, in February 2021, employees of Bryan Bass received an email inquiry from the payment processing company Paysafe directed to the sham company Lindau Pearl Group LLC, one of the trade names for Lindau Horse Polo. Paysafe indicated it had identified unusual activity on

Lindau Horse Polo's account and requested, among other items, Lindau Horse Polo's last three months of bank statements and details related to transactions on two different Visa cards. Defendant Bass forwarded the email to Defendant Smith and requested details for the two Visa transactions, indicating that when responding to Paysafe, "We can use a different number and email for the Customer so they are unable to contact the Customer."

70. If banks and payment processors knew that Defendants' sham companies would be processing other companies' payments through their merchant accounts, they likely would neither enable the sham companies to obtain merchant accounts nor allow the accounts to remain open. Indeed, when financial institutions and payment processors have learned about the scheme, they have labeled the activity as money laundering, fraud, and transaction laundering, and promptly closed the accounts and rejected applications seeking to obtain new merchant accounts.

71. For example, after the financial institution Esquire bank identified two merchant accounts as potentially engaged in money laundering, Esquire closed the accounts as well as seven additional merchant accounts that appeared to be linked to the two accounts. After additional investigation, Esquire identified 59 additional accounts associated with the original two accounts and subsequently another 38 associated accounts. Esquire closed all of these accounts. On multiple occasions, Esquire has shut down merchant accounts belonging to the scheme's sham companies due to findings of excessive declined charges or fraud. The CB Surety Defendants received notifications of these actions by Esquire.

72. When financial institutions and payment processors have detected Defendants' use of the transaction laundering tactic, financial institutions and payment processors also added the sham companies and straw owners to card networks' TMFs. This, in turn, leads other financial institutions and payment processors to close accounts held by these same sham companies and straw owners or to reject applications seeking to obtain new merchant accounts. When a sham company is detected and closed, however, Defendants typically start routing the merchant clients' transactions through one or more of the many other sham companies they control and operate.

Chargeback-Reduction Tactic

73. Defendants use the chargeback-reduction tactic to help their merchant clients maintain access to bank accounts. This tactic is used to artificially lower the merchant clients' chargeback rates by using prepaid debit cards to create sham transactions, thus inflating the number of transactions flowing through the clients' accounts that do not result in chargebacks.

74. Defendants collect large deposits from their merchant clients and use those deposits to initiate numerous small-dollar sham transactions (also called "microtransactions") that appear as if they are payments for the merchant's goods or services. The merchant, in effect, pays itself: the money it pays to Defendants as part of the large deposit is returned to it in the form of the microtransactions. For their part, Defendants collect a percentage of the transactions as a service fee. Because these sham transactions never result in returns or chargebacks, they artificially lower the merchant account's overall chargeback rate.

75. In enabling and conducting these transactions, Defendants intend to deceive financial institutions and card networks that monitor the accounts of the merchant clients, causing these entities to extend credit when they would not otherwise do so. CB Surety has utilized this tactic to deceive financial institutions on a large scale: a document stored on a CB Surety Google Drive summarizes an inventory of prepaid debit cards obtained by CB Surety from more than a dozen vendors and totaling over $180,000. In some instances, issuers of CB Surety's prepaid debit cards have become aware of use of the cards in a manner consistent with chargeback-reduction efforts and alerted CB Surety regarding this activity.

76. The chargeback-reduction tactic subjects financial institutions to the risk of loss and leads financial institutions to unwittingly facilitate the fraudulent or otherwise illegal or high-risk activities in which Defendants' merchant clients are engaged.

V. DEFENDANTS' KNOWLEDGE OF FRAUD

77. All Defendants have knowledge of and are willing and active participants in the fraudulent scheme described above. All Defendants have knowingly conspired to further the

fraud scheme and have demonstrated their understanding that they are participants in a scheme to deceive financial institutions and to harm consumer victims.

VI. HARM TO CONSUMERS AND FINANCIAL INSTITUTIONS

78. Consumers have suffered and continue to suffer financial losses from Defendants' wire and bank fraud scheme. Those victimized by the scheme reside across the United States, including in this District.

79. Federally insured financial institutions are also harmed by Defendants' wire and bank fraud scheme in several ways. First, both issuing banks and acquiring banks risk forfeiting the dollar amount of the chargebacks that Defendants' merchant clients incur using fraudulently obtained and maintained merchant accounts. Further, the acquiring banks that Defendants deceive may incur financial penalties imposed by card networks by unknowingly permitting Defendants to process payments for merchant clients engaged in fraudulent, illegal, or high-risk activities. The banks may also incur reputational harm.

80. For example, Esquire Bank and U.S. Bank, both financial institutions as defined in 18 U.S.C. § 20 and 18 U.S.C. § 1344, during their due diligence process identified sham companies created by Defendants. Both banks closed the sham companies' merchant accounts immediately to avoid facilitating any illegal business, incurring any financial penalties, and suffering reputational harm. Even after the closure of these accounts, however, Defendants continued to hold merchant accounts in the name of other sham companies at Esquire Bank and U.S. Bank.

81. Defendants are continuing to pursue the fraud scheme. Absent injunctive relief by this Court, Defendants' conduct will continue to cause injury to financial institutions and consumers across the United States and victims may be denied the opportunity to obtain restitution.

COUNT 1

(18 U.S.C. § 1345 – Injunctive Relief)

82. The United States re-alleges and incorporates by reference Paragraphs 1 through 81 of this Complaint as though fully set forth herein.

83. By reason of the conduct described herein, all Defendants have violated, are violating, and are about to violate 18 U.S.C. §§ 1343 and 1349 by conspiring to execute and executing a scheme and artifice to defraud for obtaining money by means of false or fraudulent representations with the intent to defraud, and, in so doing, using interstate and foreign wire communications.

84. By reason of the conduct described herein, all Defendants have violated, are violating, and are about to violate 18 U.S.C. §§ 1344 and 1349 by conspiring to execute and executing a scheme and artifice to defraud financial institutions and by conspiring to execute and executing a scheme and artifice to obtain moneys owned by, or under the custody or control of, financial institutions, by means of false or fraudulent pretenses, representations, or promises.

85. Upon a showing that Defendants are committing, conspiring to commit, or about to commit wire fraud or bank fraud, the United States is entitled, under 18 U.S.C. § 1345, to seek a preliminary injunction and a permanent injunction restraining all future fraudulent conduct and ordering any other action that the Court deems just to prevent a continuing and substantial injury.

86. As a result of the foregoing, Defendants' conduct should be enjoined, and Defendants should be prevented from dissipating and concealing their ill-gotten gains.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff United States of America requests of the Court the following relief:

87. That the Court issue an order, pursuant to 18 U.S.C. § 1345, pending a hearing and determination of the United States' application for a preliminary injunction, that Defendants, their agents, officers and employees, and all other persons or entities in active concert or participation with them, are temporarily restrained from:

a. committing wire fraud, as defined by 18 U.S.C. § 1343;

b. committing bank fraud, as defined by 18 U.S.C. § 1344;

c. conspiring to commit wire and bank fraud, as defined by 18 U.S.C. § 1349;

d. charging, causing others to charge, or aiding others in charging unauthorized debits against bank accounts;

e. defrauding consumers, financial institutions, and others, in any way;

f. incorporating or exercising control over any additional corporate entities in furtherance of the fraud scheme;

g. alienating or disposing of assets that are the proceeds of the fraud scheme or are used or planned to be used in any way to further the fraud scheme; and

h. destroying, deleting, removing, or transferring any and all records of any nature related to the Defendants' business, financial, or accounting operations.

88. That the Court issue an order, pursuant to 18 U.S.C. § 1345, pending a hearing and determination of the United States' application for a preliminary injunction, freezing Defendant Thomas Eide's and Defendant Smith's assets.

89. That the Court issue an order, pursuant to 18 U.S.C. § 1345, pending a hearing and determination of the United States' application for a preliminary injunction, freezing the assets of Defendants CB Surety LLC, Peak Bakery LLC, Cascades Pointe at Clemson, LLC, KP Testing, LLC, Motion Media Marketing Inc., SJC Financial Services Inc., Reseller Consultants, Inc., Ambragold, Inc., Think Processing LLC, and Bass Business Consultants—including any assets in bank accounts held by these defendants or controlled by these defendants, as well as any assets in bank accounts held by others "doing business as" these defendants or vice versa.

90. That the Court issue an order, pursuant to 18 U.S.C. § 1345, pending a hearing and determination of the United States' application for a preliminary injunction, appointing a temporary receiver over Defendants CB Surety LLC, Peak Bakery LLC, Cascades Pointe at Clemson, LLC, KP Testing, LLC, Motion Media Marketing Inc., SJC Financial Services Inc., Reseller Consultants, Inc., Ambragold, Inc., Think Processing LLC, and Bass Business

Consultants, as well as any other entities these defendants, Defendant Eide, or Defendant Smith control.

91. That the Court issue preliminary injunctions on the same basis to the same effect.

92. That the Court issue permanent injunctions on the same basis and to the same effect.

93. That the Court order such other and further relief as the Court shall deem just and proper.

Dated: December 1, 2023

Respectfully submitted,

PHILLIP A. TALBERT
United States Attorney

TARA AMIN
Assistant United States Attorney

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General

ARUN G. RAO
Deputy Assistant Attorney General

AMANDA N. LISKAMM
Director, Consumer Protection Branch

RACHAEL L. DOUD
Assistant Director, Consumer Protection Branch

ANDREW K. CRAWFORD
FRANCISCO L. UNGER
Trial Attorneys
United States Department of Justice

Attorneys for Plaintiff United States of America